

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
12 April 2001 (12.04.2001)

PCT

(10) International Publication Number
WO 01/26284 A1

(51) International Patent Classification⁷: H04L 12/24. (29/06)

(21) International Application Number: PCT/FI00/00810

(22) International Filing Date: 21 September 2000 (21.09.2000)

(25) Filing Language: Finnish

(26) Publication Language: English

(30) Priority Data: 19992056 24 September 1999 (24.09.1999) FI

(71) Applicant (for all designated States except US): ELISA COMMUNICATIONS OYJ [FI/FI]; Korkeavuorenkatu 35-37, FIN-00130 Helsinki (FI).

(72) Inventor; and

(75) Inventor/Applicant (for US only): JUHOLA, Arto [FI/FI]; Helsinginkatu 9 B 36, FIN-00500 Helsinki (FI).

(74) Agent: SEppo LAINE OY; Itämerenkatu 3 B, FIN-00180 Helsinki (FI).

(81) Designated States (national): AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

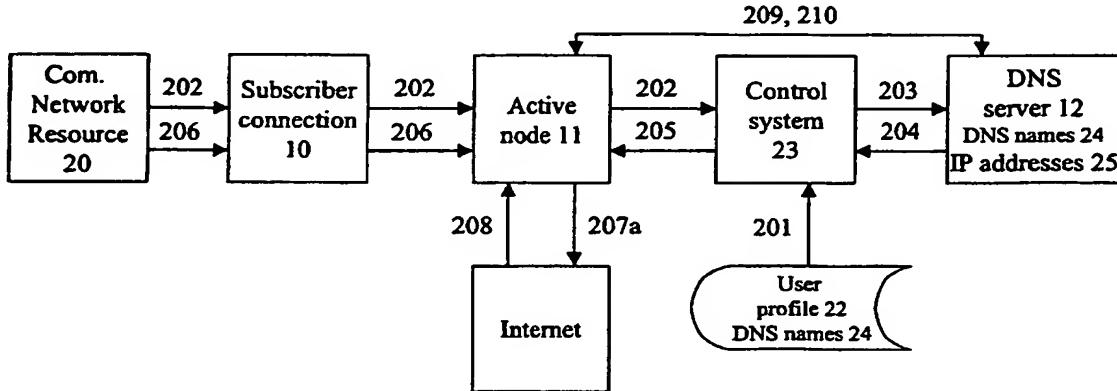
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

- With international search report.
- Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.

[Continued on next page]

(54) Title: METHOD FOR CONTROLLING TRAFFIC IN A DATA NETWORK



WO 01/26284 A1

(57) Abstract: The invention relates to a method for traffic control in a communications network, in which method the transmission of a data packet to its destination address is inhibited on the basis of the source or destination address of the data packet and in which method bindings defined between middleware-level and network-level information are utilized in traffic control at the network-level so that the traffic flow in the communications network can be controlled on the basis of barring lists at the middleware level. The invention is based on combining Internet middleware facilities with programmable active networks and/or routers. An automatic monitoring system is configured so that traffic outbound from a given subscriber connection and targeted to another given subscriber connection is passed via the traffic monitoring system. Herein, a precompiled middleware-level name list is utilized wherefrom the middleware-level names used by said given subscriber connection are selected (201) to form a barring list. On the basis of the thus formed middleware-level barring list, into the monitoring system by way of reading the response messages of a name server system is compiled (205) a network-level barring list, whose addresses are maintained valid not longer than the validity time indicated in the response message of the name server system, thus accomplishing the novel technique of traffic control on the basis of a subscriber-specific middleware-level barring list.



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method for controlling traffic in a data network

5 The invention relates to a method according to the preamble of claim 1 for traffic control in a communications network, in which method the transmission of a data packet to its destination address is inhibited on the basis of the source or destination address of the data packet and in which method bindings defined between middleware-level and network-level information are utilized in traffic control at the network-level.

10 In communications networks, the data flow therethrough is divided into hierarchical levels. Traffic at a given level of the hierarchical system is transparent to the elements of the other under/overlying hierarchical levels. In the context of the present application, the term middleware level is used when reference is made to levels 4-7 15 of the OSI (Open System Interconnection) model defined by ISO (International Organization for Standardization), said levels including the transport, session, presentation and application layers. Hence, middleware must be understood to represent the software that is capable of implementing the functionality of said layers.

20 One of the middleware-level protocols is the DNS according to which Internet resources are given a DNS name that does not contain the location information of the resource at the network level. Reference to resources must be made by their DNS names because of such reasons as, e.g., the IP addresses of host resources that generally are computers connected to the Internet, are not any more static, but rather, 25 may change due to dynamic IP address updates and changes occurring in the network locations of terminal equipment. Moreover, according to Internet drafts terminal users may not directly use IP addresses, but instead always their DNS names. Communications network resources that can be referred to by middleware names may also be application programs or instances thereof runnable in a communications 30 network or documents stored in a communications network.

In conventional communications networks, the transmission of inbound or outbound traffic of a network terminal from the source to the destination may be limited on the basis of network-level information, such an IP address, whereby it is possible, if so desired, to inhibit traffic emanating from or directed to certain network-level 5 addresses such as IP addresses or, alternatively, to facilitate traffic only from or to certain network-level addresses. This kind of traffic barring may be implemented with firewall techniques, for instance. A firewall is an arrangement wherein the internal network of an organization is connected to an external network via a physical monitoring device, whereby inbound traffic emanating from certain 10 network-level addresses can be barred at the firewall. Outbound traffic may be controlled in a similar manner.

A disadvantage of the prior art is that the traffic control systems of the middleware 15 level (e.g., DNS) and the network level operate independently from each other, whereby any possible traffic-limiting actions implemented at the middleware level, such as connection barring lists that contain nonpermitted originating or destination names, have no limiting effect on the network-level traffic, thus readily passing unnecessary and undesirable traffic to the unprotected network level, such as commercial mail or even spam mail sent to annoy the receiving party. Until today, no 20 solution has been presented that could effectively and dynamically combine the traffic control systems of the middleware level with those of the network level.

Closed user groups (VPN, Virtual Private Network) implemented at the middleware 25 level are not automatically recognized at the network level, which means that traffic of undesirable nature may be easily sent to the networks, or parts thereof, employed by such closed user groups of the middleware level if the sender happens to know, e.g, some DNS names or IP addresses of the group. In some cases, this may cause harm due to the limited data transfer capacity of the communications network. When undesirable traffic blocks the network, also the desired messages are hindered or 30 blocked from reaching their destinations.

The location of communications network resources may change from a given IP address to an other, whereby barring assigned to a given IP address does not bar traffic originating from another IP address of the resource.

5 There is also a need for limiting access as per connection, terminal or user to certain generally offered communications network resources on the basis of DNS names due to certain reasons such as those children's mental hygienes and other practicalities. This is not, however, possible with the tools available in the art.

10 It is an object of the invention to provide an entirely novel type of method capable of overcoming the problems of the above-described prior art. The goal of the invention is achieved by virtue of combining Internet middleware and Internet router and/or active-network techniques. Herein, the inbound and outbound traffic of a subscriber connection are passed via an automatic monitoring system. Such a monitoring

15 system can be implemented as a so-called active node or a separate router-containing server that is capable of processing the headers and data content of data packets, such as IP packets, passed through the monitoring system under dynamically loadable software. Herein, the term dynamically loadable software is used to indicate that the computer software controlling the monitoring system may be updated at any time

20 without a disturbing break in the operation of the monitoring system. Dynamic updatability is needed for making changes in the list of nonpermitted middleware-level addresses and the barring list of their corresponding network-level addresses in the automatic monitoring system and/or in the network operator system. The embodiment according to the invention uses a predetermined middleware-level name

25 policy, such as a given address space containing, e.g., all the DNS names for which a certain one or ones of name server systems can find the corresponding network-level addresses or, alternatively, a name space that contains all the names of a given middleware-level name space that are formed according to a correct syntax, such as those of the DNS, but which may not necessarily have a corresponding address at the

30 network level.

Next, an updatable subscriber-specific middleware-level name policy is defined by way of delineating a set of names from the predetermined name space. The subscriber-specific middleware-level name policy contains middleware-level names such that the communications network resources bound thereto are permitted and/or are not permitted to receive data from a given subscriber connection and/or middleware-level names such that the communications network resources bound thereto are permitted and/or are not permitted to send data to a given subscriber connection.

The subscriber-specific middleware-level name policy is stored in the automatic monitoring system, in the network operator system or otherwise accessible to the operator. The function of the invention is to intercept in the automatic monitoring system such traffic which is sent from a network-level address or is directed to a network-level address, whose communications network resource having at the very moment a bound middleware-level name that, on the basis of the subscriber-specific middleware-level name policy, is not permitted to communicate traffic. This binding between a given middleware-level name and its network-level address is decoded from the response message of a name server system and, additionally, said network-level address is not held valid longer than the validity time defined in the response message, whereby traffic can be inhibited to network-level addresses whose valid bound middleware-level addresses are unknown and, respectively, to or from communications network resources that are bound to said middleware-level names and are included in the name policy barring list.

More specifically, the method according to the invention for traffic control in a communications network is characterized by what is stated in the characterizing part of claim 1.

The invention offers significant benefits. The invention makes it possible to reduce unnecessary and undesirable traffic at the network level. Moreover, the invention facilitates compilation of barring list for communications policies based on middleware-level names such as those of the DNS or setting up closed user groups (VPN,

Virtual Private Network) at the middleware level, wherein the network-level definitions of a group are updated dynamically so as to correspond to the middleware-level definition of the group so as to maintain a correspondence of the middleware-level names of the group with the valid bound names thereof at the network level.

5

By virtue of the invention, the network operator and users are offered a facility to inhibit traffic from a selected subscriber connection to such communications network resources that are bound to middleware-level names whose respective bound network-level addresses have not been queried by request message to a name server system from said subscriber connection during a given period of time. The method may also be applied so that therein is defined at least one network-level address or, alternatively, a group of addresses whereto sent or wherfrom emanating traffic is accepted even if the respective network-level address has not been retrieved from a name server system during a given period of time.

10

In the method, the network level can undergo an automatic reconfiguration so that it continually supports the configuration of the overlying level. Hence, if traffic is defined barred for a given DNS name or set of names, also the respective traffic directed to an IP address or address space bound to said name or name policy is barred without a separate reconfiguration of IP-address-based barring lists, whereby all traffic directed to or emanating from given network-level addresses will be inhibited based on said DNS name policy.

20

By virtue of the method, it is possible on the basis of the DNS name policy to inhibit traffic to certain network resources that are commonly known to be available in communications networks as per connection, terminal or user when such reason as those related to children's mental hygienes and other practicalities are concerned.

25

In the following, the invention is examined in detail with the help of exemplifying embodiments by making reference to the attached drawings.

30

There are two basic application of the invention to a TCP/IP environment, both of them being capable of operating in parallel:

5 FIG. 1 is a block diagram representing barring of outbound IP traffic to addresses that are unknown to the DNS and/or are included in name policy barring list; and

FIG. 2 is a block diagram representing barring of undesirable IP traffic through automatic and active transfer of middleware-level traffic control configuration policy to the network level.

10 Referring to FIG. 1, the technique shown therein for barring outbound IP traffic to addresses unknown to the DNS and/or are included in barring list of nonpermitted names uses the elements described below and performs the steps described later in the text. In this exemplifying embodiment, a given one or given ones of name server systems are assumed to be capable of carrying out name resolution for the predetermined name policy, wherein said predetermined name policy comprises the entire name space, whose syntax covers the name space for which a given one or given ones of name server systems are capable of performing a name resolution, but within which a given single one of the names of the name space need not necessarily have a corresponding bound network-level address, and in which a subscriber-specific set of middleware-level names forms a name space for which a given name server system is capable of retrieving the corresponding bound network-level addresses. The exemplifying embodiment is herein described using the DNS as the name server system and, respectively, the predetermined middleware-level name policy is assumed to be formed by syntactically correct DNS names. Correspondingly, the subscriber-specific middleware-level name set is assumed to comprise such names for which the DNS can perform a name resolution on the basis of a DNS request message sent from a subscriber connection 10.

15

20

25

30 The subscriber connection 10 is essentially a so-called Stub Internet that only connects the user network to an active node 11. The active node 11 is a communications

network element incorporating software that monitors the header information of IP packets inbound to the active node 11 and controls the routing of IP packets. The active node 11 is located so that all network traffic to the subscriber connection 10 passes through the node. The arrangement used in the exemplifying embodiment also 5 makes it possible to use a limited subset of the subscriber-specific middleware-level name policy. Herein, in the active node 11 is stored a name policy barring list comprising the permitted and/or nonpermitted DNS names that can be dynamically updated under a control issued, e.g., from the network operator system or the subscriber connection 10. DNS request messages sent from the subscriber connection 10, which generally are directed to the DNS, are passed to a DNS server 12.

The method is implemented by way of the steps described below. Steps 101 - 102 are carried out to inhibit a name server system from receiving requests issued from the subscriber connection 10 toward the name server system on such DNS names that 15 are bound to communications network resources not permitted to have an access from the subscriber connection 10:

- 101) Active node 11 receives from subscriber connection 10 a request directed to DNS server 12 on a desired DNS name 13.
- 20 102) The request on the desired DNS name 13 is forwarded (102a) from the active node 11 to the DNS server 12 if the requested DNS name 13 is an unconditionally permitted name or is included in the group of permitted names in middleware level barring list. Otherwise, the request on the desired DNS name 25 will not be forwarded and the list of permitted names in the middleware name policy will not be updated. Herein, to the user host operating from the subscriber connection 10 will be sent (102b) a DNS response message emanating from the source address of the DNS server 12 and containing a message information that the requested DNS name does not exist or, 30 alternatively, containing a more appropriate error information.

The next steps are carried out if the request on the desired DNS name is forwarded to the DNS server 12. Step 103 is carried out to update the active node to accept traffic to such a communications network resource bound to such a DNS name for which traffic is permitted. Step 103 is needed to ensure correct execution of step 104 and step 105 can be executed independently from the other steps.

5

103) Active node 11 receives a response message from DNS server 12 as a reply to the request sent in step 101. If the response message contains the requested DNS name 13 and the respective requested IP address 14 bound thereto, as well as the validity time 15 of the binding between said address and the DNS name 13 in the TTL field of the message, the requested IP address 14 is updated as a permitted address in the name policy barring list stored in the active node. The active node 11 is herein activated to accept traffic to the IP address 14 bound to the requested DNS name 13, however, not longer than the validity time 15 of the binding. The response message received from the DNS server 12 is forwarded from the active node to the user host operating from the subscriber connection 10.

10

15

20 Next the active node receives a first message directed from the user host operating the Stub Internet, or the subscriber connection 10, to the requested IP address 14 in step 104 and/or, in step 105, a second message directed to a nonpermitted IP address.

25

104) In active node 11 is received a first message directed from the user host operating the subscriber connection 10 to the requested IP address 14, whereby the active node logic checks possible information linked on the barring list to the requested IP address 14 and forwards the first message if there is validity time 15 left.

30

105) In active node 11 is received a second message 18 directed from the subscriber connection 10 to a nonpermitted IP address, whereby the active node logic checks the permission state of the nonpermitted address 17, finds the address

nonpermitted and inhibits the forwarding of the message.

To relieve the active node 11 from storing an excessively vast amount of information, the original validity times in the TTL fields may be replaced by shorter times, whereby permitted addresses may be removed from the name policy stored in the active node 11 at an accelerated rate. DNS requests sent from the subscriber connection 10 can be routed via, e.g., a Token-Bucket traffic controller, whereby it is possible to limit the number of DNS requests sent by a given subscriber during a given period of time, thus extending the maximum possible storage time of network-level addresses in the active node 11, as well as the time allowable for the system reconfiguration according to the information conveyed by the received DNS message.

Now referring to FIG. 2, therein is shown another exemplifying embodiment capable of reducing undesired IP traffic by virtue of automatic and active transfer of the middleware-level traffic control configuration policy to the network level.

Herein, an active node 11 programmed to read messages sent from a DNS server 12 is located so that all network traffic to a first subscriber connection 10 passes therethrough. A communications network resource 20, such as a user host, communicates with the communications network via a subscriber connection. In the diagram, control system 23 refers to a network operator system wherefrom the operator can provide communications network connections for communications network resources operating via the network operator clients' subscriber connections. DNS names 24 may be any kind of names compatible with the DNS syntax. IP addresses 25 are such IP addresses that are stored bound to the DNS names 24 in the DNS. User profile 22 includes definitions that are stored in the operator's network management system or, alternatively, in a separate control system serving as subsystem of such a network management system 23, so as to define the services offered to a given data network user or data network resource. The method is carried out by way of performing the following steps denoted by reference numbers. Step

201 is carried out to delineate the set of DNS addresses wherefrom traffic to a given subscriber connection is permitted or whereto data transmission from a given subscriber connection is permitted.

5 201) In network control system 23 is defined for at least one given communications network resource, such as a user host, the set of DNS names permitted for use. The definition of the name policy can be made entirely or partially by the operator or the client, in a static manner, or, in a dynamic manner during an ongoing communications session between the communications network resource 20 and the operator's control system. The names may be stored in any physical place that can be made accessible to the operator's control system 23. Also accessible to the operator's control system 23, there is compiled, as per each communications network resource separately, a user profile that facilitates the search of permitted DNS names.

15 Steps 202 - 205 are carried out to link a given user or terminal with a first subscriber connection 10 and to inform the active node 11 monitoring said subscriber connection on possible traffic constraints associated with said given user or said given terminal. In these steps, a subscriber-connection-specific middleware-level name policy, denoted as DNS names 24 in the diagram, is used to search for one name or a greater number of names of the policy such a bound network-level address, IP addresses 25, whose validity time can be verified from a reply message of a name server system, whereupon each one of retrieved addresses is separately defined as a permitted address and/or nonpermitted address so that the bound addresses of nonpermitted middleware-level names are respectively defined as nonpermitted network-level addresses and/or the bound addresses of permitted middleware-level names are respectively defined as permitted network-level addresses in the monitoring system of the node.

30 202) Communications network resource 20, such as a user host, is registered to operate under user profile 22 on a communications connection established via

a subscriber connection 10, and information on the registration is submitted to operator's control system 23.

203) Control system 23 sends a request message to a DNS, e.g., from a DNS 5 server 12, pertaining to such IP addresses 25 bound to DNS names 24 that are permitted to communicate inbound and/or outbound traffic with a given connection operating under a given user profile 22, the connection in the diagram being a subscriber connection 10.

10 204) Control system 23 receives at the active node 11 a reply message or a number of reply messages from the DNS pertaining to the requested DNS names 24 and their bound IP addresses 25, complemented with information on the validity time of the bindings between said DNS names 24 and said IP addresses 25.

15 205) Active node 11 receives from control system 23 the IP addresses 25 submitted by the DNS, together with the validity times of the IP addresses, and the IP addresses 25 with their validity times are stored pairwise with their bound names as permitted addresses on the barring list stored in the active node 11.

20 Later after these steps, the control system takes care of requesting the valid IP addresses bound to the DNS names 23 and their respective validity times from the DNS and forwards this information to the active node 11. As trigger for such requests serve the validity times of the IP addresses 25 received earlier from the 25 name server system or, alternatively, trigger times shorter than those. Resultingly, a DNS request is sent separately per each DNS name 23 before the lapse of the validity time associated with any DNS name 23. Furthermore, IP addresses 25 can be canceled from the list of permitted IP addresses of the name policy stored in the active node using such a trigger associated with their validity times that any IP address will be canceled not later than at the end of its validity time.

In steps 206 - 207 of the method, the active node receives a data packet and, when necessary, inhibits forwarding. Obviously, these steps may also be carried out preceding steps 204 - 205, but in this case no further data transmission can take place.

- 5 206) At the active node 11 is received a third message outbound from the subscriber connection 10 to the IP address to be verified or, respectively, a third message sent from the IP address to be verified to the subscriber connection 10, whereupon the logic of the active node 11 checks whether the IP address 26 to be verified is a permitted IP address included in the list of valid permitted addresses of the barring list stored in active node 11.
- 10
- 207) The third message is sent (207a) in the communications network forward toward the destination address or subscriber connection 10 defined in the third message in the case that the IP address to be verified is found on the list of valid permitted addresses of the name policy stored in active node 11. If not so, the third message is intercepted at the active node 11.
- 15

When the subscriber-connection-specific middleware-level barring list is formed based on an extensive DNS name policy, the traffic received outbound from the subscriber connection 10 can be handled by means of the first exemplifying embodiment, whereby there is no need to configure the active node 11 to store all the bound IP addresses of the subscriber-connection-specific middleware-level barring list, but instead it is sufficient to dynamically update only those addresses to which the user's terminal device launches DNS requests via the active node 11 and, as reply messages to said requests, such information is received that, on the basis of the subscriber-connection-specific middleware-level barring list, is considered necessary to be stored in the active node 11.

To monitor extensive DNS name sets of traffic passed from a communications network via the active node 11 and, particularly such traffic that is inbound to the subscriber connection 10, steps 208 - 210 described below must be carried out. The

technique described herein makes it also possible to monitor such DNS names of communications network resources toward which outbound traffic from the subscriber connection 10 emanates. In the subsequent steps, the monitoring system receives a given data packet directed to a communications network resource 20 or emanating from a subscriber connection, whereupon a request is sent to a name server system to retrieve the network-level source address to be verified for said data packet and/or a given middleware-level name bound to the destination address of the packet, after which the operator system checks whether said middleware-level name can be found in the subscriber-connection-specific middleware-level name policy and, as a result of the check that may indicate said given middleware-level name either being or not being defined in the subscriber-connection-specific middleware-level name policy, the network-level source and/or destination address can be defined as a permitted or nonpermitted address in the monitoring system. If steps 208 - 210 are carried out, step 205 is redundant, and steps 206 - 207 may also be carried out prior to steps 208 - 210 and/or after these steps.

208) Active node 11 receives a data packet containing a source and/or destination IP address which is not defined *a priori* in the network-level barring list stored in the active node 11 and thus needs verification.

209) Triggered by the received data packet's IP address that requires verification, a so-called reverse-DNS query, initiated by the logic of the active node 11 or controlled by said active node, is sent wherein the bound DNS name of the received IP address is requested from a DNS system, such as DNS server 12.

210) Active node 11 and/or the operator's control system 23 receives the response message sent by the DNS. Next, a check is performed whether the DNS named bound to the IP address to be verified can be found on the list of permitted DNS names that, depending on the case, may be located in the control system 23, made available to the control system 23 or stored in the active node 11. If the bound DNS name is found on the list of permitted DNS names, the active

node 11 is controlled to pass the data packet traffic to the IP address thus verified, however, not longer than the validity time defined in the TTL field referring to the verified IP address in the response message pertaining to the IP address to be verified.

5

In step 210, it is important to have a fast configuration update of the name policy if the data packets are desired to be forwarded to the destination address prior to the receipt of the response message to the reverse query, that is, without subjecting the data packet to address verification. Herein, one solution is to limit the handling rate of the subscriber-connection-specific DNS requests by means of a traffic controller. However, the forwarding of a short burst of data to a subscriber connection is not a risk as serious as that caused by network flooding, e.g., during a "denial of service" attack. Moreover, the adverse effects of nonverified data transmissions can be alleviated by means of limiting the volume of traffic inbound from addresses not yet subject to verification or outbound to unverified destination addresses. This arrangement can be implemented by way of, e.g., directing such traffic to a dedicated Token-Bucket queue. Then, the volume limitation of the traffic can be eased after the address verification step is completed.

20

The invention may also be applied so that, in addition to or as an alternative of the name policy of permitted DNS names, which is maintained in the operator's control system 23 and/or in the active node 11, there is maintained a policy of nonpermitted DNS names, whereby the traffic can be controlled based thereon.

25

A still another approach to the application of the invention is such that the active node 11 is configured with the subscriber-connection-specific middleware-level name policy, such as permitted DNS names, and the logic of the active node 11 is allowed to communicate requests to the DNS pertaining to the IP addresses bound to the names of the policy and the validity times of the names of the policy, in practice by requesting the contents of the TTL fields, the requests being triggered by earlier received validity times.

A further another approach to the application of the invention is such that the network-level barring lists are set, in accordance with barring lists defined for the respective bound middleware-level names, to cover certain combinations of source and destination addresses in data packets, whereby the combinations include at least one network-level source and destination address also in the case that the received data packet contains a plurality of source and/or destination addresses. This arrangement makes it possible to intercept the forwarding of a data packet on the basis of a given route defined for the packet.

10

Another further possible application of the invention is such that, a message defined to be intercepted on the basis of some barring list criteria, is diverted to an exceptional route, whereby the access of the message to its destination address is inhibited also in the case that the message is not intercepted by the monitoring system.

15

The method according to the invention can avail of the facilities offered by Secure DNS in order to monitor that requests sent to the DNS are actually sent by such a communications network resource which is allocated to perform policy configurations upon such requests and that the response messages of the name server system 20 actually are responses to such requests.

The following definitions are given to clarify the meaning of certain terms used in the present application and particularly in the appended claims.

25 Monitoring system means apparatus which is connected in a communications network on the operator's side in regard to the operator interface with a subscriber connection and serves to control traffic in the communications network. A monitoring system may comprise a programmable active node, server or other communications network element or a system connected to a communications network with capabilities of reading network-level source and/or destination address information 30 contained in inbound data packets and of comparing address information of inbound

data packets with network-level address information stored in the monitoring system and, on the basis of the results of such a comparison, of sending the received data packet forward from the monitoring system or, respectively, of intercepting the received data packet in the monitoring system. Monitoring system may also mean a 5 system fulfilling the above definitions and having middleware-level names stored therein. Such a system is capable of sending a reverse DNS request pertaining to given network-level address information to a name server system or network operator's control system and of receiving given middleware-level name information bound to given network-level address information and of comparing given 10 middleware-level name information with subscriber-connection-specific name policy maintained in the monitoring system or made available to the monitoring system, said policy containing at least one permitted and/or one nonpermitted middleware-level name for the use of said subscriber connection. As a response to a comparison performed on a middleware-level name, the subscriber-connection-specific address 15 policy maintained in the monitoring system may be updated with a given network-level address, and traffic which is coming from a given network-level source address, is directed to a given network-level destination address or is intended to pass via a route of predetermined addresses to its final destination address. Obviously, the monitoring system may also be implemented as a software portion of 20 the network operator's control system.

User profile includes definitions that are stored in a network operator's control system or are available to a separate control system acting as a subsystem to the operator's control system, whereby the definitions serve to define the services 25 offered to a given communications network user or resource. User profile may also contain information on intercept policy covering the blocking of inbound traffic to a given subscriber connection from any communications network resource listed in the middleware-level name policy and/or of outbound traffic from said given subscriber connection to any communications network resource listed in the middleware-level 30 name policy.

The term name is used in communications systems when reference is made to a symbolic identifier, such as the URN (Uniform Resource Name) for instance, which has no location-dependent portion. The term name also used in the present context when reference is made to, e.g., the DNS host name that on one hand represents the 5 name of a resource location inasmuch a host is seen by abstract resources as a location and, on the other hand, is also required to have a name that is independent from the network-level address, such as the IP address.

10 Name server and name server system refer to a system capable of submitting information assigned to a middleware-level name at the receipt of the middleware-level name. Herein, the assigned information may include, e.g., the network-level bound address corresponding to a given middleware-level name and the validity time of the binding between such a given middleware-level name and its bound network-level address.

15 Resource and communications network resource refer to a subscriber connection, a user host connected thereto, application software and/or an instance thereof runnable on an information network.

20 Network-level bound address is a bound address that at the network level represents a given middleware-level name to which the network-level address is assigned at a given instant of time; in other words, a communications network resource having said given middleware-level name is at said given instant of time accessible at said network-level address that in the context of the present application and particularly 25 in the claims appended thereto is called the network-level bound address.

Cancellation from a barring list means inactivation of a definition from a policy, whereinafter said definition no longer exists as a traffic constraint in the policy.

30 Request generation refers to compilation of a request message or content fields of messages by means of the logic of the message-generating system.

Binding between a network-level address and its bound middleware-level name and, conversely, binding between a middleware-level name and its bound network-level address refers to a definition stored in a name server system that binds said 5 middleware-level name with said given network-level address.

What is claimed is:

1. Method of traffic control in a communications network, in which method the transmission of a data packet to its destination address is barred on the basis of the source or destination address of the data packet, the method comprising the steps of
 - 5 - defining (205) at least one permitted and/or nonpermitted network-level source and/or destination address into a barring list of a network-level policy,
 - passing (206) a data packet inbound to a subscriber connection (10) or
 - 10 - outbound from a subscriber connection (10) via an automatic monitoring system (11) incorporated in a network operator's control system, and
 - barring (207) the forwarding of said data packet to its destination address as a system response to a comparison performed between at least one network-level source address and/or destination address included in said barring list with at
 - 15 - least one source and/or destination address of said data packet,

c h a r a c t e r i z e d in that

- a predetermined middleware-level name space is used,
 - from said predetermined middleware-level name space is delineated (201) a subset of subscriber-connection-specific middleware-level names containing at least one permitted and/or nonpermitted middleware-level source and/or destination name, and said subset is stored, at least by those portions not yet stored, in a form available to the network operator's system,
 - on the basis of the thus defined policy of subscriber-connection-specific middleware-level names, there is defined (205) at least one network-level address bound to at least one name in the policy of subscriber-connection-specific middleware-level names as a nonpermitted network-level address and, each network-level address bound to a permitted middleware-level name is defined as a permitted network-level address in the barring list of network-level policy stored in a monitoring system, and

5 - the thus defined network-level addresses, which are bound in the network-level policy stored in said monitoring system to the respective names in the policy of subscriber-connection-specific middleware-level names, are canceled automatically from the network-level policy not later than at the end of the validity time of the binding between any network-level address and its bound middleware-level name.

10 2. Method according to claim 1, characterized by the steps of

15 - receiving (208) in said monitoring system a given data packet destined to said subscriber connection or sent from said subscriber connection and retrieving from a name server system for a traffic control check a given middleware-level name which is bound to the network-level source and/or destination address of said data packet,

20 - checking (209) in the operator's system whether said retrieved bound middleware-level name can be found in said policy of subscriber-connection-specific middleware-level names, and

25 - as a result of said given middleware-level name either being or not being defined in the subscriber-connection-specific middleware-level name policy, defining (209) said network-level source and/or destination address subjected to the verification check as a permitted or nonpermitted address.

30 3. Method according to any one of claims 1 - 2, characterized by the step of

 - retrieving (203 - 204), on the basis of the predetermined subscriber-connection-specific middleware-level name policy, for at least one name of said subscriber-connection-specific middleware-level name policy such a network-level bound address whose validity time can be decoded from a response message of said name server system, and defining (205) each one of such retrieved network-level bound addresses separately as a permitted address and/or nonpermitted address so that the bound addresses of nonpermitted middleware-level names are respectively defined as nonpermitted network-level addresses and/or the bound addresses of permitted middleware-level

names are respectively defined as permitted network-level addresses in the monitoring system.

4. Method according to any one of claims 1 - 3, characterized in that
5 said network-level bound address to be included in the barring list is retrieved (203 – 204) from said name server system by means of sending at least one request directed to the name server system, generated by the network operator's system and pertaining to at least one name of said subscriber-connection-specific middleware-level name policy, and saved in response messages concerning each one of said
10 requested middleware-level names.

5. Method according to claim 4, characterized in that at least one of the requests generated by said network operator's system is generated in the monitoring system.

15 6. Method according to any one of claims 1 - 5, characterized in that said predetermined middleware-level name space comprises all the middleware-level names for which a given name server system or given ones of name server systems are capable of performing a name resolution and that said subscriber-connection-specific middleware-level name policy comprises all the permitted and/or nonpermitted source addresses for a data packet to be forwarded to said given subscriber connection and/or all the permitted and/or nonpermitted destination addresses for a data packet to be sent from said given subscriber connection.

25 7. Method according to any one of claims 1 - 5, characterized in that said given name server system or given ones of name server systems are capable of performing a name resolution for the names of said predetermined middleware-level name space and that said predetermined middleware-level name space comprises the entire name space, whose syntax covers the name space for which said given one or
30 given ones of name server systems are capable of performing a name resolution, but within which name space a given single one of the names of said name space need

not necessarily have a corresponding bound network-level address, and in which name space a subscriber-specific middleware-level policy forms a name subspace for which a given name server system is capable of retrieving the corresponding bound network-level addresses.

5

8. Method according to any one of claims 1 - 7, characterized by the steps of

- receiving in the monitoring system a response message from said name server system, the message being destined to said subscriber connection (10) and indicating the requested network-level bound address of said given name of said subscriber-connection-specific middleware-level name policy, and
- as a system response to the received response message, defining said network-level bound address decoded from said response message as a permitted address in the barring list stored in said monitoring system.

15

9. Method according to any one of claims 1 - 8, characterized in that said given name server system is a DNS or a part thereof and that the network-level addresses and network-level bound addresses are IP addresses and that the middleware-level names bound to these addresses are DNS names.

20

10. Method according to any one of claims 1 - 9, characterized in that said monitoring system is implemented by means of a programmable active node (11).

25

11. Method according to any one of claims 1 - 10, characterized in that outbound messages directed from said subscriber connection toward said name server system are diverted to a traffic controller that forwards the messages to said name server so as to prevent the number of messages sent from said subscriber connection to said name server from exceeding a given limit value during a given period of time.

30

12. Method according to any one of claims 1 - 11, characterized in that said

subscriber-connection-specific middleware-level name policy is defined (201) on the basis of a user profile assigned to said subscriber connection (10).

13. Method according to any one of claims 1 - 12, characterized in that
5 access of traffic to a given network-level address is granted when said given network-level address is a permitted address and/or traffic is blocked to a given network-level address is granted when said given network-level address is a nonpermitted address, however, not longer than the validity time indicated in the response message of the name server system for the binding between said network-
10 level address and said given middleware-level name bound thereto, unless a new response message is received from said name server system pertaining to said given network-level address and indicating a longer validity time of said given network-level address.

15 14. Method according to claim 13, characterized in that the maximum value of said validity time is set equal to the validity time indicated in the TTL field of the DNS response message that contains the information on the binding between said given network-level address and said given middleware-level name bound thereto.

20 15. Method according to any one of claims 1 - 14, characterized in that the trigger for sending a request to said name server system pertaining to said given middleware-level name is selected to be the remainder value of the validity time of the binding between said given network-level address and said given middleware-level name bound thereto.

25

16. Method according to any one of claims 1 - 15, characterized by the steps of

- receiving (101) in said monitoring system a request message directed from said subscriber connection (10) toward said name server system (12) pertaining to a given middleware-level name, and
- as a response to the received request message, comparing said given

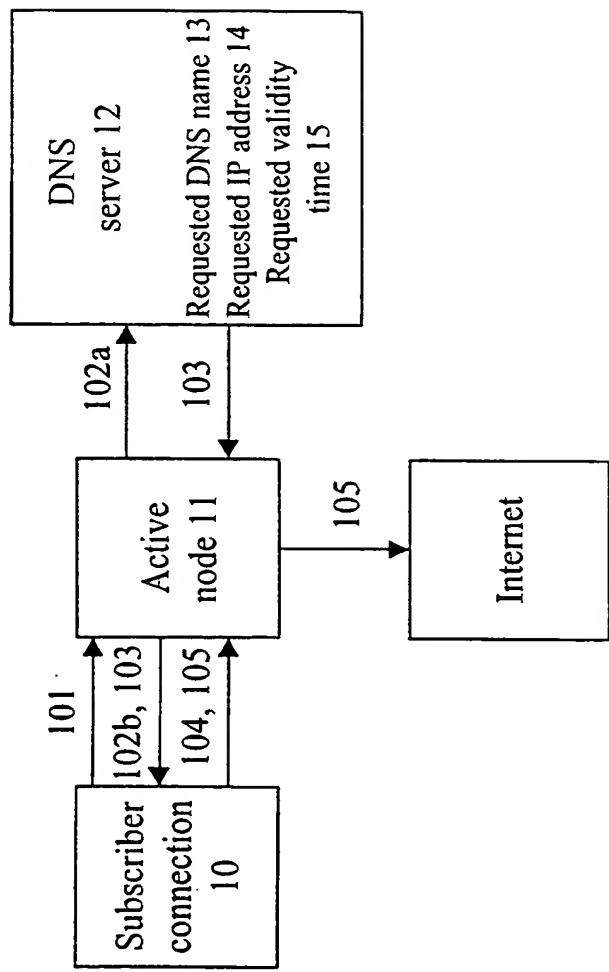
30

middleware-level name with said subscriber-connection-specific middleware-level name policy, and when necessary barring (102) the request from reaching said name server system.

5 17. Method according to any one of claims 1 - 16, characterized in that at least one data packet is barred from reaching its destination address by way of intercepting said packet in the monitoring system as response of at least one of it's source and/or destination addresses.

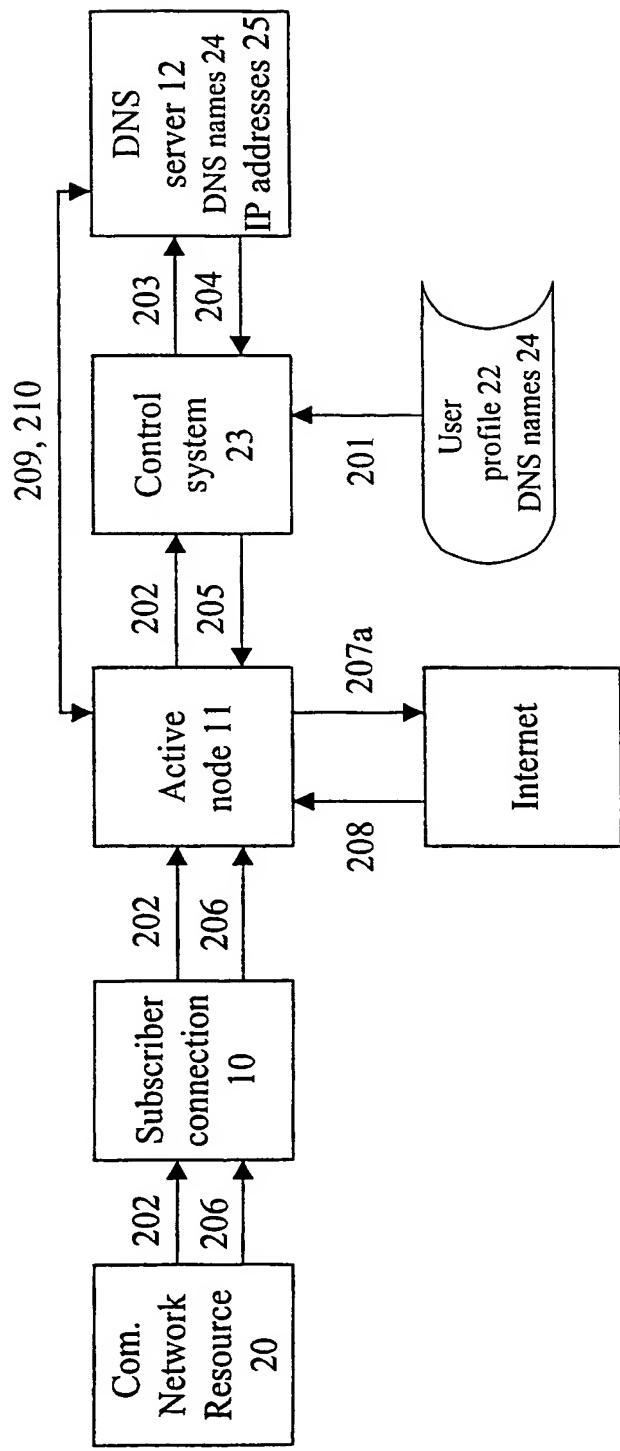
1/2

Fig. 1



2/2

Fig. 2



INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI 00/00810

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/24, H04L 29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9930460 A2 (SUN MICROSYSTEMS, INC.), 17 June 1999 (17.06.99), the whole document --	1-17
A	WO 9916202 A2 (COMBER, CURTIS T. ET AL), 1 April 1999 (01.04.99), page 1, line 8 - page 2, line 26; page 7, line 14 - page 9, line 31, claims 1-13, abstract --	1-17
A	WO 9859470 A2 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 30 December 1998 (30.12.98), the whole document --	1-17

 Further documents are listed in the continuation of Box C. See patent family annex.

- * Special categories of cited documents
- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "I," document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed
- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search

2 March 2001

Date of mailing of the international search report

02-03-2001

Name and mailing address of the ISA/
Swedish Patent Office
Box 5055, S-102 42 STOCKHOLM
Facsimile No. + 46 8 666 02 86

Authorized officer

Roger Bou Faisal /OGU
Telephone No. + 46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI 00/00810

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0909072 A2 (LUCENT TECHNOLOGIES INC.), 14 April 1999 (14.04.99), the whole document --	1-17
A	SE 9702389-9 L (TELIA AB), 24 December 1998 (24.12.98), abstract -----	1

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI 00/00810

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
WO	9930460	A2	17/06/99	AU	1811599 A	28/06/99

WO	9916202	A2	01/04/99	AU	1062499 A	12/04/99
				AU	9582798 A	12/04/99
				AU	9582998 A	12/04/99
				AU	9583198 A	12/04/99
				AU	9583298 A	12/04/99
				AU	9583398 A	12/04/99
				AU	9583598 A	12/04/99
				AU	9583698 A	12/04/99
				AU	9584098 A	12/04/99
				AU	9666398 A	12/04/99
				AU	9667198 A	12/04/99
				AU	9667298 A	12/04/99
				AU	9667598 A	12/04/99
				AU	9667698 A	12/04/99
				AU	9667898 A	12/04/99
				AU	9667998 A	12/04/99
				AU	9668098 A	12/04/99
				AU	9668298 A	03/05/99
				AU	9777098 A	12/04/99
				AU	9777298 A	12/04/99
				AU	9777398 A	12/04/99
				EP	1015970 A	05/07/00
				EP	1015986 A	05/07/00
				EP	1015995 A	05/07/00
				US	6032184 A	29/02/00
				US	6115040 A	05/09/00
				WO	9915950 A	01/04/99
				WO	9915960 A	01/04/99
				WO	9915974 A	01/04/99
				WO	9915975 A	01/04/99
				WO	9915977 A	01/04/99
				WO	9915978 A	01/04/99
				WO	9915979 A	01/04/99
				WO	9915984 A	01/04/99
				WO	9915988 A	01/04/99
				WO	9915989 A	01/04/99
				WO	9915996 A	01/04/99
				WO	9916002 A	01/04/99
				WO	9916099 A	01/04/99
				WO	9916198 A	01/04/99
				WO	9916203 A	01/04/99
				WO	9916206 A	01/04/99
				WO	9916207 A	01/04/99
				WO	9916218 A	01/04/99
				WO	9916230 A	01/04/99
				WO	9919803 A	22/04/99

WO	9859470	A2	30/12/98	AU	8052398 A	04/01/99
				SE	9702385 A	24/12/98

EP	0909072	A2	14/04/99	JP	11163940 A	18/06/99
				US	6141749 A	31/10/00

SE	9702389-9	L	24/12/98	NONE		

THIS PAGE BLANK (USPTO)